ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ
ПО СТАНДАРТИЗАЦИИ

**Р 1323565.
1.010—
2017**

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование функции диверсификации для формирования производных ключей платежного приложения

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАНЫ Обществом с ограниченной ответственностью «Системы практической безопасности» (ООО «СПБ») совместно с Открытым акционерным обществом «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС») и Обществом с ограниченной ответственностью «КРИПТО-ПРО» (ООО «КРИПТО-ПРО»)

2 ВНЕСЕНЫ Техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации»

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 декабря 2017 г. № 2018-ст

4 ВВЕДЕНЫ ВПЕРВЫЕ

*Правила применения настоящих рекомендаций установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящим рекомендациям публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящих рекомендаций соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2018

Настоящие рекомендации не могут быть полностью или частично воспроизведены, тиражированы и распространены в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и обозначения 1
3.1 Термины и определения 1
3.2 Обозначения 2
4 Описание алгоритмов 3
4.1 Вывод мастер-ключей платежного приложения карты 3
4.2 Вывод сессионных ключей платежного приложения карты 3
4.3 Вывод мастер-ключей платежного приложения карты для персонализации 4
Приложение А (справочное) Контрольные примеры 5

Введение

В настоящих рекомендациях рассмотрены три подсистемы порождения производных ключей: подсистема порождения мастер-ключей платежного приложения карты для использования на этапе персонализации; подсистема порождения мастер-ключей карты из мастер-ключей банка-эмитента для использования на этапе процессинга; подсистема порождения сессионных ключей карты, используемых на этапе процессинга, из мастер-ключей карты.

Во всех случаях для порождения ключей использована функция диверсификации ключа KDF_GOSTR3411_2012_256, описанная в Р 50.1.113—2016 (далее — KDF).

Разработка настоящих рекомендаций вызвана необходимостью внедрения процедур для порождения производных ключей платежных приложений.

Примечание — Настоящие рекомендации дополнены приложением А.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование функции диверсификации для формирования производных ключей платежного приложения

Information technology. Cryptographic data security.
Using the key diversification function to generate payment application derived keys

Дата введения — 2018—06—01

1 Область применения

Описанные в настоящих рекомендациях алгоритмы рекомендуется применять для реализации механизмов обеспечения безопасности информации в платежной системе «МИР».

2 Нормативные ссылки

В настоящих рекомендациях использована нормативная ссылка на следующий документ:

Р 50.1.113—2016 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования

Примечание — При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных документов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный документ, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого документа с учетом всех внесенных в данную версию изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то рекомендуется использовать версию этого документа с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и обозначения

3.1 Термины и определения

В настоящих рекомендациях применен следующий термин с соответствующим определением:

3.1.1 **машина персонализации:** Машина электрической персонализации, предназначенная для первичной загрузки ключевой и служебной информации в чип карты.

Издание официальное

3.2 Обозначения

В настоящих рекомендациях использованы следующие обозначения:

V_n — конечномерное векторное пространство размерности n;

$A||B$ — конкатенация строк, т. е. если $A \in V_{n1}$, $B \in V_{n2}$, $A = (a_{n1-1}, a_{n1-2}, ..., a_0)$, $B = (b_{n2-1}, b_{n2-2}, ..., b_0)$, то $A||B = (a_{n1-1}, a_{n1-2}, ..., a_0, b_{n2-1}, b_{n2-2}, ..., b_0) \in V_{n1+n2}$;

AC — прикладная криптограмма (Application Cryptogram), формируемая картой. Длина значения равна 8 байтам;

ATC — счетчик транзакций (Application Transaction Counter). Длина счетчика равна 2 байтам;

CSN — серийный номер чипа (Chip Serial Number). Длина значения равна 4 байтам;

$HMAC_{256}$ — функция вычисления кода аутентификации сообщения HMAC, использующей алгоритм HMAC_GOSTR3411_2012_256, описанный в Р 50.1.113—2016. Длина значения равна 32 байтам;

IMK — мастер-ключ эмитента (IMK_{AC}, IMK_{SMI}, IMK_{SMC} или IMK_{IDN}), используемый в качестве ключа диверсификации функции KDF в соответствии с Р 50.1.113—2016 для формирования мастер-ключей карты. Длина значения равна 32 байтам;

K_{ENC} — мастер-ключ карты, используемый для генерации сессионного ключа S_{ENC} формирования/проверки криптограммы приложения карты и криптограммы машины персонализации; после персонализации удаляются. Длина значения равна 32 байтам;

K_{MAC} — мастер-ключ карты, используемый для генерации сессионного ключа S_{MAC} для обеспечения целостности обмена между картой и машиной персонализации (вычисления имитовставки); после персонализации удаляются. Длина значения равна 32 байтам;

K_{DEC} — мастер-ключ карты, используемый для генерации сессионного ключа S_{DEC} для шифрования и расшифрования конфиденциальных данных, передаваемых в команде персонализации; после персонализации удаляются. Длина значения равна 32 байтам;

KDF — функция диверсификации, использующая алгоритм KDF_GOSTR3411_2012_256, описанный в Р 50.1.113—2016. Длина значения равна 32 байтам;

KEYDATA — данные для формирования ключей карты $KMC_{ID}||CSN$. Длина значения равна 10 байтам;

KMC — ключ эмитента, используемый для формирования ключей персонализации, в качестве ключа диверсификации функции *KDF* в соответствии с Р 50.1.113—2016, а также для формирования мастер-ключей карты для персонализации. Длина значения равна 32 байтам;

KMC_{ID} — идентификатор *KMC*. Длина значения равна 6 байтам;

label — некоторая константа, значение которой равно *label* = (0*x*21||0*x*07||0*x*22||0*xe*6). Длина значения равна 4 байтам;

*label*1 — некоторая константа, значение которой равно *label*1 = (0*x*21||0*x*07||0*x*22||0*xe*7). Длина значения равна 4 байтам;

*label*2 — некоторая константа, значение которой равно *label*2 = (0*x*21||0*x*07||0*x*22||0*xe*8).Длина значения равна 4 байтам;

*label*3 — некоторая константа, значение которой равно *label*3 = (0*x*21||0*x*07||0*x*22||0*xe*9). Длина значения равна 4 байтам;

MK — мастер-ключ карты (MK_{AC}, MK_{SMI}, MK_{SMC} или MK_{IDN}). Длина значения равна 32 байтам;

MK_{AC} — мастер-ключ карты, используемый для вычисления прикладной криптограммы; используется в качестве ключа диверсификации функции *KDF* в соответствии с Р 50.1.113—2016 для формирования сессионных ключей карты SK_{AC}. Длина значения равна 32 байтам;

MK_{SMI} — мастер-ключ карты, используемый для обеспечения целостности передаваемых в скриптовой команде данных и аутентификации источника данных команды; используется в качестве ключа диверсификации функции *KDF* в соответствии с Р 50.1.113—2016 для формирования сессионных ключей карты SK_{SMI}. Длина значения равна 32 байтам;

MK_{SMC} — мастер-ключ карты, используемый для обеспечения конфиденциальности передаваемых в скриптовой команде данных; используется в качестве ключа диверсификации функции *KDF* в соответствии с Р 50.1.113—2016 для формирования сессионных ключей карты SK_{SMC}. Длина значения равна 32 байтам;

MK_{IDN} — мастер-ключ карты, используемый для вычисления *IDN* (ICC Dynamic Number) при динамической аутентификации карты. Длина значения равна 32 байтам;

PAN — номер карты (Primary Account Number). Длина значения равна от 12 до 20 десятичных цифр;

PAN Sequence Number — порядковый номер карты (владельца), если к счету привязано более одной карты. Длина значения равна 1 байту и имеет формат XX, где X — десятичная цифра.

R — вектор диверсификации. Длина значения равна 8 байтам;

SK_{AC} — сессионный ключ, используемый картой и эмитентом для формирования криптограмм ARQC и ARPC (вычисление имитовставки). Длина значения равна 32 байтам;

SK_{SMI} — сессионный ключ, используемый для обеспечения целостности скриптовых команд, т. е. для формирования имитовставки. Длина значения равна 32 байтам;

SK_{SMC} — сессионный ключ, используемый для обеспечения конфиденциальности данных скриптовых команд (разблокировка или смена PIN), т. е. для шифрования данных команды. Длина значения равна 32 байтам.

4 Описание алгоритмов

Возможные значения аргументов функций в представленных алгоритмах ограничены допустимостью их использования в качестве входных параметров преобразований.

4.1 Вывод мастер-ключей платежного приложения карты

Формирование мастер-ключа карты *MC* (MK_{AC}, MK_{SMI}, MK_{SMC} или MK_{IDN}) осуществляется с использованием функции диверсификации KDF_GOSTR3411_2012_256 на основе $HMAC_{256}$ и определяется выражением

$MK = KDF(K_{in}, label, seed) = HMAC_{256}(K_{in}, 0x01||label||0x00||seed||0x01||0x00)$,

где

$K_{in} = IMK$

$label = (0x21||0x07||0x22||0xe6)$

$seed = Y$;

Y равен 16 правым десятичным цифрам *X*, если *X* менее 16 цифр, то *X* дополняется до 8 байт нулями;

X = *PAN*||*PAN Sequence Number* (если *PAN Sequence Number* отсутствует, то его значения заменяется нулями),

т. е.

$MK = HMAC_{256}(IMK, 0x01||label||0x00||Y||0x01||0x00)$

4.2 Вывод сессионных ключей платежного приложения карты

4.2.1 Вывод сессионного ключа для вычисления прикладной криптограммы

Формирование сессионного ключа карты SK_{AC} осуществляется с использованием функции диверсификации KDF_GOSTR3411_2012_256 на основе $HMAC_{256}$ и определяется выражением

$SK_{AC} = KDF(K_{in}, label, seed) = HMAC_{256}(K_{in}, 0x01||label||0x00||seed||0x01||0x00)$,

где

$K_{in} = MK_{AC}$

$label = (0x21||0x07||0x22||0xe6)$

$seed = R$

$R = ATC||0xf0||0x00||0x00||0x00||0x00||0x00||0x00$,

т. е.

$SK_{AC} = HMAC_{256}(MK_{AC}, 0x01||label||0x00||R||0x01||0x00)$

4.2.2 Вывод сессионного ключа для обеспечения целостности передаваемых в скриптовой команде данных и аутентификации источника данных команды — эмитента

Формирование сессионного ключа карты SK_{SMI} осуществляется с использованием функции диверсификации KDF_GOSTR3411_2012_256 на основе $HMAC_{256}$ и определяется выражением

$SK_{SMI} = KDF(K_{in}, label, seed) = HMAC_{256}(K_{in}, 0x01||label||0x00||seed||0x01||0x00)$,

где

$K_{in} = MK_{SMI}$

$label = (0x21||0x07||0x22||0xe6)$

seed = *R*
R = *AC*,
т. е.
$SK_{SMI} = HMAC_{256}$ (MK_{SMI}, 0*x*01||*label*||0*x*00||R||0*x*01|0*x*00)

4.2.3 Вывод сессионного ключа для обеспечения конфиденциальности передаваемых в скриптовой команде данных

Формирование сессионного ключа карты SK_{SMC} осуществляется с использованием функции диверсификации KDF_GOSTR3411_2012_256 на основе $HMAC_{256}$ и определяется выражением
$SK_{SMC} = KDF(K_{in}, label, seed) = HMAC_{256}(K_{in}, 0x01||label||0x00||seed||0x01||0x00)$,
где
$K_{in} = MK_{SMC}$
label = (0*x*21||0*x*07||0*x*22||0*xe*6)
seed = *R*
R = *AC*,
т. е.
$SK_{SMC} = HMAC_{256}$ (MK_{SMC}, 0*x*01||*label*||0*x*00||R||0*x*01|0*x*00)

4.3 Вывод мастер-ключей платежного приложения карты для персонализации

Формирование мастер-ключа карты K_{ENC} осуществляется с использованием функции диверсификации KDF_GOSTR3411_2012_256 на основе $HMAC_{256}$ и определяется выражением
$K_{ENC} = KDF(K_{in}, label1, seed) = HMAC_{256}(K_{in}, 0x01||label1||0x00||seed||0x01||0x00)$,
где
K_{in} = *KMC*
*label*1 = (0*x*21||0*x*07||0*x*22||0*xe*7)
seed — последние 8 байт KEYDATA
seed = *Z*,
т. е.
$K_{ENC} = HMAC_{256}$ (KMC, 0*x*01||*label*1||0*x*00||Z||0*x*01||0*x*00)

Формирование мастер-ключа карты K_{MAC} осуществляется с использованием функции диверсификации KDF_GOSTR3411_2012_256 на основе $HMAC_{256}$ и определяется выражением
$K_{MAC} = KDF(K_{in}, label2, seed) = HMAC_{256}(K_{in}, 0x01||label2||0x00||seed||0x01||0x00)$,
где
K_{in} = *KMC*
*label*2 = (0*x*21||0*x*07||0*x*22||0*xe*8)
seed — последние 8 байт KEYDATA
seed = *Z*,
т. е.
$K_{MAC} = HMAC_{256}$ (*KMC*, 0*x*01||*label*2||0*x*00||Z||0*x*01||0*x*00)

Формирование мастер-ключа карты K_{DEC} осуществляется с использованием функции диверсификации KDF_GOSTR3411_2012_256 на основе $HMAC_{256}$ и определяется выражением
$K_{DEC} = KDF(K_{in}, label3, seed) = HMAC_{256}(K_{in}, 0x01||label3||0x00||seed||0x01||0x00)$,
где
K_{in} = *KMC*
*label*3 = (0*x*21||0*x*07||0*x*22||0*xe*9)
seed — последние 8 байт *KEYDATA*
seed = *Z*,
т. е.
$K_{DEC} = HMAC_{256}$ (*KMC*, 0*x*01||*label*3||0*x*00||Z||0*x*01||0*x*00)

Приложение А
(справочное)

Контрольные примеры

Приводимые ниже значения параметров *PAN*, *PAN Sequence Number*, *ATC*, *AC*, *KEYDATA*, а также значения ключей эмитента *KMC*, IMK_{AC}, IMK_{SMI}, IMK_{SMC}, IMK_{IDN} рекомендуется использовать только для проверки корректной работы конкретной реализации алгоритмов, описанных в настоящих рекомендациях.

Все числовые значения приведены в десятичной или шестнадцатеричной записи. Нижний индекс в записи числа обозначает основание системы счисления. Представление числа из десятичной системы счисления в шестнадцатеричный вид происходит по следующему правилу: каждые две цифры десятичного числа переводят в двузначное шестнадцатеричное число, например целое число 1213456789_{10} представляется в шестнадцатеричном виде, как число $0c0d2d4359_{16}$.

В данном приложении двоичные строки из V^*, длина которых кратна 4, записываются в шестнадцатеричном виде, а символ конкатенации («||») опускается. То есть строка $a \in V_{4r}$ будет представлена в виде $a_{r-1}\ a_{r-2} \ldots a_0$, где $a_i \in \{0, 1, \ldots, 9, a, b, c, d, e, f\}$, $i = 0, 1, \ldots, r - 1$. Соответствие между двоичными строками длины 4 и шестнадцатеричными строками длины 1 задается естественным образом (таблица А.1).

Преобразование, ставящее в соответствие двоичной строке длины $4r$ шестнадцатеричную строку длины r, и соответствующее обратное преобразование для простоты записи опускаются.

Таблица А.1 — Соответствие между двоичными и шестнадцатеричными строками

0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	a
1011	b
1100	c
1101	d
1110	e
1111	f

А.1 Исходные данные

PAN = 123456789012345671_{10}
PAN_Sequence_Number = 95_{10}
ATC = $df6c_{16}$
AC = $9f64235a71ddee5b_{16}$
CSN = $994c551e_{16}$
$KMC_{ID} = fd5645a58b76_{16}$
KEYDATA = $fd5645a58b76994c551e_{16}$
KMC = 000102030405060708090a0b0c0d0e0f\\
101112131415161718191a1b1c1d1e1f$_{16}$

IMK_{AC} = 000102030405060708090*a*0*b*0*c*0*d*0*e*0*f*\\
101112131415161718191*a*1*b*1*c*1*d*1*e*11$_{16}$
IMK_{SMI} = 000102030405060708090*a*0*b*0*c*0*d*0*e*0*f*\\
101112131415161718191*a*1*b*1*c*1*d*1*e*12$_{16}$
IMK_{SMC} = 000102030405060708090*a*0*b*0*c*0*d*0*e*0*f*\\
101112131415161718191*a*1*b*1*c*1*d*1*e*13$_{16}$
IMK_{IDN} = 000102030405060708090*a*0*b*0*c*0*d*0*e*0*f*\\
101112131415161718191*a*1*b*1*c*1*d*1*e*14$_{16}$

Символ «\\» обозначает перенос числа на новую строку.

А.1.1 Мастер-ключи платежного приложения карты

MK_{AC} = *fb*9*fb*1*c*1*cbf*367*fc*4*c*4*f*872*a*360*b*907*f*\\
18*f*78964*efffd*714*d*972738*b*47*f*935*d*9$_{16}$
MK_{SMI} = *d*37*cf*9*fc*1*d*60*e*200200*c*0*ace*0*a*4*e*7*adc*\\
*aaa*9176*acde*1*a*1*e*9*cd*5*d*2*ea*3679628*ad*$_{16}$
MK_{SMC} = *d*02037*c*2*e*074*d*3867*a*517*b*5058*fe*3887\\
0*d*320*ff*8156*eccd*2*f*9*dc*27*cefad*05*e*27$_{16}$
MK_{IDN} = 4*ea*368*db*926*da*5*b*101*c*32*d*34*f*0*b*24803\\
53*db*104*e*44*dd*57*df*907*e*00594*b*299*dcd*$_{16}$

А.1.2 Сессионные ключи платежного приложения карты

SK_{AC} = 5361*ad*354*b*17186*e*09*deb*20*d*37586*d*46\\
*a*64*f*8*cddd*699238*f*0210*db*7*d*9*e*6090*ed*$_{16}$
SK_{SMI} = 4*b*6*af*8*f*777*c*5001*d*6*ae*570*d*29*b*9*d*1*b*60\\
43777887*c*1*cc*4*db*64*feaa*8*ba*0*a*226788$_{16}$
SK_{SMC} = 6*a*0*cd*3673*c*2*ce*5*e*8*f*32*c*5*c*6698829917\\
665*ff*5*b*8920750*fcec*465*c*2*ddc*271*c*14$_{16}$

А.1.3 Мастер-ключи платежного приложения карты для персонализации

K_{ENC} = 239*ae*6*ef*90*a*1*ebd*1*fbc*2*a*3*cf*695*e*6*f*10\\
*bfd*1*b*2*da*6*e*73*e*04*dc*5*b*76*de*4*aa*7*ac*544$_{16}$
K_{MAC} = 3*d*292*eecd*26*b*7963*b*4*c*980*d*5*fcd*3068*f*\\
624*b*6*d*56*b*434326*d*89*cdf*5842*b*193006$_{16}$
K_{DEC} = *ce*9*ec*8*c*79*b*8*a*679*b*2*b*12*bf*5514143*b*5*a*\\
9*a*805*fd*615*f*801*b*2*b*856921*ddd*216130$_{16}$

А.2 Исходные данные

PAN = 6789012345673$_{10}$
PAN_Sequence_Number = 93$_{10}$
ATC = 125*a*$_{16}$
AC = 1234567871*ddee*5*b*$_{16}$
CSN = 994*c*5512$_{16}$
KMC_{ID} = *fd*5645938*b*76$_{16}$
KEYDATA = *fd*5645938*b*76994*c*5512$_{16}$
KMC = 000102030405060708090*a*0*b*0*c*0*d*0*e*0*f*\\
101112131415161718191*a*1*b*1*c*1*d*1*e*0*f*$_{16}$
IMK_{AC} = 000102030405060708090*a*0*b*0*c*0*d*0*e*0*f*\\
101112131415161718191*a*1*b*1*c*1*d*1*e*21$_{16}$
IMK_{SMI} = 000102030405060708090*a*0*b*0*c*0*d*0*e*0*f*\\
101112131415161718191*a*1*b*1*c*1*d*1*e*22$_{16}$
IMK_{SMC} = 000102030405060708090*a*0*b*0*c*0*d*0*e*0*f*\\
101112131415161718191*a*1*b*1*c*1*d*1*e*23$_{16}$
IMK_{IDN} = 000102030405060708090*a*0*b*0*c*0*d*0*e*0*f*\\
101112131415161718191*a*1*b*1*c*1*d*1*e*24$_{16}$

А.2.1 Мастер-ключи платежного приложения карты

MK_{AC} = 91*bca*45*ae*14*ce*443*d*88*e*99*bc*407*ac*829\\
7*d*6*d*1953094*ff*48*c*5116*ce*8*f*08*d*964*ca*$_{16}$
MK_{SMI} = *f*64*ff*9474739*b*93*e*7*e*9*d*6*bd*2*ef*3669*fb*\\
1*ae*8*c*0*ad*9*b*2*bc*5*eaa*180*dcdff*7*d*95101$_{16}$
MK_{SMC} = 8*c*0928*f*2791*be*89202*b*2*e*5165571*cd*96\\
*a*360*bc*256*b*27815547*c*7*fa*3*ae*9*bdaa*14$_{16}$

MK_{IDN} = 23df44a5dd9e2c755504dc4c736427b8\\
6478841d8fea535fb09c34a1410f3097$_{16}$

А.2.2 Сессионные ключи платежного приложения карты

SK_{AC} = 04f9b88df553d190a2aeb2f4d9f2b6a2\\
f4ce8eac89eab879a807866c0ec0e6f8$_{16}$

SK_{SMI} = 88f8163b91e53ccd1d42e5aed806b2f2\\
aa022e3b558051642ead998c5e1af330$_{16}$

SK_{SMC} = c7d8fc5f9cb04f9b86f30f0f6e40188a\\
f9513abe0ffd684261d89424f6c4680a$_{16}$

А.2.3 Мастер-ключи платежного приложения карты для персонализации

K_{ENC} = 63b47cd8e6b3743946f279be412e9f87\\
19013ee919ab99ee0b253cd5f5c43978$_{16}$

K_{MAC} = d5f40f395712ec4e47540318b5b718eb\\
8bb195994ff10e7c6e4a896760f443f7$_{16}$

K_{DEC} = 0f17df77467bcc4deef2c016eed30753\\
2d337d21f5ed1295234528a4c9fe1fc7$_{16}$

А.3 Исходные данные

PAN = 98765432112341$_{10}$

PAN_Sequence_Number = 98$_{10}$

ATC = 126c$_{16}$

AC = 0998235a71ddee5b$_{16}$

CSN = 104c551e$_{16}$

KMC_{ID} = fd5645a51276$_{16}$

KEYDATA = fd5645a51276104c551e$_{16}$

KMC = 000102030405060708090a0b0c0d0e0f\\
101112131415161718191a1b1c1d1e3d$_{16}$

IMK_{AC} = 000102030405060708090a0b0c0d0e0f\\
101112131415161718191a1b1c1d1e31$_{16}$

IMK_{SMI} = 000102030405060708090a0b0c0d0e0f\\
101112131415161718191a1b1c1d1e32$_{16}$

IMK_{SMC} = 000102030405060708090a0b0c0d0e0f\\
101112131415161718191a1b1c1d1e33$_{16}$

IMK_{IDN} = 000102030405060708090a0b0c0d0e0f\\
101112131415161718191a1b1c1d1e34$_{16}$

А.3.1 Мастер-ключи платежного приложения карты

MK_{AC} = d8f6180a5e1b909ad222f137c7385811\\
a869ef6a67c156296a8419d6f337ad14$_{16}$

MK_{SMI} = 3b8fd0a39151b2fba7ad72ca7fbda0ad\\
62ce02d74ae00e3aff24b2221b5f83ca$_{16}$

MK_{SMC} = 298027ce6608a6b26b3c9157dd0457da\\
4f144a7c4b471e5306f40793db04ed73$_{16}$

MK_{IDN} = 326236064be404964d716c47db6b8dab\\
75d9cb0cb599db240c782db8fa140ac7$_{16}$

А.3.2 Сессионные ключи платежного приложения карты

SK_{AC} = ed7e91da7485ca6324ae0e982d699e1e\\
3bf74df8a4691c231ab5d378c02f4367$_{16}$

SK_{SMI} = dca82274bd029bbe9e4265af9651de4a\\
c61b55c3bc4f862f057d3ed549ce15b3$_{16}$

SK_{SMC} = 3aee3354c808edd7f3bca1f77186f86b\\
550748cebe0882e072e7294f6a9660e5$_{16}$

А.3.3 Мастер-ключи платежного приложения карты для персонализации

K_{ENC} = 8f6fe73189b70614d518d8bc56759578\\
58da3b9825ddb705787cff81d57ec81d$_{16}$

K_{MAC} = 9ce94350c5e9b9f835888f6065956efb\\
a6133ad1fba2fc31303caae56e6ea6ea$_{16}$

K_{DEC} = cadf60b985e8ca702a98e49ab4ed53b5\\
5ed1e7d2adaeae46cb1c3e2efb7607bb$_{16}$

УДК 681.3.06:006.354 ОКС 35.040

Ключевые слова: информационная технология, криптографическая защита информации, аутентификация, ключ, функция диверсификации, платежная карта, платежное приложение

БЗ 1—2018/92

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Поповой*

Сдано в набор 20.12.2017. Подписано в печать 14.02.2018. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,26. Тираж 19 экз. Зак. 102.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
gost.e-ecolog.ru gost.e-ecolog.ru

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123001, Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru